# Short Laws for Finite Groups and Residual Finiteness Growth

Henry Bradford and Andreas Thom

**Abstract**

We prove that for every $n \in \mathbb{N}$ and $\delta > 0$ there exists a word $w_n \in F_2$ of length $O(n^{2/3}\log(n)^{3+\delta})$ which is a law for every finite group of order at most $n$. This improves upon the main result of [24] by the second named author. As an application we prove a new lower bound on the residual finiteness growth of non-abelian free groups.

## 1 Introduction

A *law* for a group $G$ is an equation which holds identically in $G$. The qualitative study of laws in groups is a classical subject, often phrased in terms of *varieties of groups,* [21, 22]. Moreover certain specific laws have been the subject of intense study over the years, particularly power laws, which delineate the territory of the *bounded* and *restricted Burnside problems.* A more recently opened avenue of research has been the asymptotic behaviour of lengths of laws for sequences of finite groups, motivated by connections with other invariants of interest in asymptotic group theory.

### 1.1 Statement of Results

Our focus in this paper will be on the length of laws which are satisfied *simultaneously* by all sufficiently small finite groups. Our main result is as follows.

**Theorem 1.1.** *For all $n \in \mathbb{N}$ there exists a word $w_n \in F_2$ of length*

$$O\left(n^{2/3}\log(n)^3\log^*(n)^2\right)$$

*such that for every finite group $G$ satisfying $|G| \leq n$, $w_n$ is a law for $G$.*

In the statement of the previous theorem, $\log^*(n)$ denotes the iterated logarithm, i.e. the smallest natural number $k$, such that the $k$-fold application of $\log\colon (0,\infty) \to (-\infty,\infty)$ to $n$ yields a real number less than 1. Note that $\log^*(n)$ grows slower than any iteration of logarithms.

The precise definition of a *law* for a group is given in Subsection 2.1. Theorem 1.1 improves asymptotically on the result of [24], in which the second named author obtained an upper bound of

$$O\left(n \log\log(n)^{9/2} / \log(n)^2\right).$$

Our second result, which is a direct application of Theorem 1.1, is a new lower bound on the residual finiteness growth of nonabelian free groups. Recall that a group $\Gamma$ is *residually finite* if, for every $1_\Gamma \neq g \in \Gamma$, there exists a finite group $H$ and a homomorphism $\pi\colon \Gamma \to H$ such that $\pi(g) \neq 1_H$. Bou-Rabee [2] introduced a quantitative version of this property, as follows. Given a residually finite group $\Gamma$ and $1_\Gamma \neq g \in \Gamma$, we define:

$$k_\Gamma(g) = \min\{|H| \mid \text{there exists } \pi\colon \Gamma \to H, \pi(g) \neq 1_H\}.$$

Now, given a generating set $S$ for $\Gamma$, there is a naturally associated length function on $\Gamma$. For $n \in \mathbb{N}$, let $B_S(n) \subseteq \Gamma$ be the set of elements of length at most $n$. We define:

$$\mathcal{F}_\Gamma^S(n) = \max\{k_\Gamma(g) \mid 1_\Gamma \neq g \in \Gamma, g \in B_S(n)\}.$$

Informally, we may think of groups $\Gamma$ for which $\mathcal{F}_\Gamma^S(n)$ grows slowly as being those in which non-trivial elements are "easy" to detect in finite quotients. Now, $\mathcal{F}_\Gamma^S$, being defined in terms of the generating set $S$, is not an invariant of $\Gamma$ alone. However, if $\Gamma$ is finitely generated, then $\mathcal{F}_\Gamma^S$ turns out to be independent of $S$ up to the equivalence relation induced by a natural partial order $\preceq$ on functions, which we make precise below. Thus we can speak without ambiguity about the *residual finiteness growth* of $\Gamma$. Since the introduction of this notion, particular attention has been paid to the task of estimating $\mathcal{F}_\Gamma^S$ for the nonabelian free groups $F_k$ ($k \geq 2$), starting with Bou-Rabee's original paper [2], and continuing through a series of papers by various authors [3, 17, 24]. Since $F_k$ has a very rich family of finite quotients, one expects its residual finiteness growth to be very slow. Consequently, any significant lower bounds on $\mathcal{F}_{F_k}^S$ represent a surprising group-theoretic phenomenon. There is a clear connection between such lower bounds and laws for finite groups: a non-trivial element $w \in F_k$ of length $n$ which is a law for all finite groups of order at most $f(n)$ witnesses that $\mathcal{F}_{F_k}^S(n) > f(n)$. From this observation, Theorem 1.1 immediately implies the following new lower bound on the residual finiteness growth of $F_k$.

**Theorem 1.2.** $\mathcal{F}^S_{F_k}(n) \succeq n^{3/2}/\log(n)^{9/2+\varepsilon}$.

It is likely that the conclusion of Theorem 1.2 is best possible up to logarithmic factors: following on from work of Hadad [12], Kassabov and Matucci ([17], Remark 9) propose that the shortest non-trivial law satisfied simultaneously by the groups $SL_2(R)$, as $R$ varies over all finite commutative rings with $|R| \leq N$, should be of length $\Omega(N^2)$. They further note that, if this conjecture is correct, then $\mathcal{F}^S_{F_k}(n) \preceq n^{3/2}$.

## 1.2 Background

The first result on residual finiteness growth of free groups appeared in Bou-Rabee's original paper introducing the notion (see also Rivin [23]).

**Theorem 1.3** ([2])**.** $\mathcal{F}^S_{F_k}(n) \preceq n^3$.

This result is an immediate consequence of a corresponding theorem on the residual finiteness growth of linear groups, via the embedding of $F_k$ into $\mathrm{SL}_2(\mathbb{Z})$. Theorem 1.3 implies that a law holding simultaneously in all finite groups of order at most $n$ must have length $\Omega(n^{1/3})$. To date these are the best complementary bounds to Theorem 1.1 and 1.2.

The first attempt to investigate the problem addressed by Theorem 1.1 was made by Bou-Rabee and McReynolds, though their result is again phrased in terms of residual finiteness growth.

**Theorem 1.4** ([3])**.** $\mathcal{F}^S_{F_k}(n) \succeq n^{1/3}$.

Theorem 1.4 implies that there exists a word $w_n$ of length $O(n^3)$ satisfying the conclusion of Theorem 1.1. Note that this already improves dramatically over the obvious laws $w_n = x^{n!}$ and say $w'_n = x^{\mathrm{lcm}(1,\ldots,n)}$ that merely show $\mathcal{F}^S_{F_k}(n) \succeq \log(n)$. Bou-Rabee and McReynolds' construction was refined by Kassabov and Matucci, who obtained the following.

**Theorem 1.5** ([17])**.** *For all $n \in \mathbb{N}$, there exists a word $w_n \in F_2$ of length $O(n^{3/2})$ such that for every finite group $G$ satisfying $|G| \leq n$, $w_n$ is a law for $G$. Consequently $\mathcal{F}^S_{F_k}(n) \succeq n^{2/3}$.*

As discussed above, prior to the present paper the best upper bound for the lengths of the $w_n$ was the following result of the second author.

**Theorem 1.6** ([24])**.** *For all $n \in \mathbb{N}$, there exists a word $w_n \in F_2$ of length*

$$O(n \log\log(n)^{9/2}/\log(n)^2)$$

*such that for every finite group $G$ satisfying $|G| \leq n$, $w_n$ is a law for $G$.*

The proof of this last result differs significantly from those which had preceded it, in that it makes extensive use of deep results from finite group theory, including the Classification of Finite Simple Groups.

It was a great surprise to the authors to discover that the main term $n$ appearing in the bound from Theorem 1.6 was not best possible. Indeed it was conjectured in [24] that it should be. In a related vein, Kassabov and Matucci asked the following.

**Question 1.7** ([17])**.** *For $k \geq 2$, is it the case that $\mathcal{F}^S_{F_k}(n) \simeq n$?*

Although Theorem 1.6 already implies a negative answer to Question 1.7 (by the observations from our Subsection 2.3, it follows from Theorem 1.6 that $\mathcal{F}^S_{F_k}(n) \succeq n \log(n)^{2-\epsilon}$), until our work it remained eminently plausible that linear bounds for $\mathcal{F}^S_{F_k}(n)$ and the length of the shortest words $w_n$ satisfying the conclusion of Theorems 1.1 and 1.6 could not be beaten by more than a polylogarithmic factor. The fact that polynomial improvements could be achieved was quite unexpected.

As regards individual groups, much recent attention has been devoted to the length of laws for simple groups. For the symmetric (and therefore also alternating) groups, the best known upper bound is provided by a result of Kozma and the second author.

**Theorem 1.8** ([20])**.** *There exists a law for* $\mathrm{Sym}(n)$ *of length at most:*

$$\exp(O(\log(n)^4 \log\log(n))).$$

If $G$ is a finite group of Lie type, then the best available bound appears in another paper of the authors.

**Theorem 1.9** ([4])**.** *Let $G$ be a finite group of Lie type over a field of order $q$, such that the natural module for $G$ has dimension $d$. Then there is a word $w_G \in F_2$ of length:*

$$q^{\lfloor d/2 \rfloor} \log(q)^{O_d(1)}$$

*which is a law for $G$.*

Furthermore, the exponent $\lfloor d/2 \rfloor$ of $q$ in Theorem 1.9 is known to be sharp: Hadad [12] gives a lower bound of $\Omega(q^{\lfloor d/2 \rfloor})$ for the length of the shortest law for $\mathrm{SL}_d(q)$, using an embedding of $\mathrm{SL}_2(q^{\lfloor d/2 \rfloor})$. Thus, the worst case is $\mathrm{SL}_2$ – a reoccuring theme in finite group theory. The same phenomenon will appear in our study of laws for all groups up to size $n$.

We will employ Theorem 1.9 in the proof of Theorem 1.1. As such a few words on the proof of Theorem 1.9 are in order. The proof strategy was inspired by that of Theorem 1.8: in both cases the problem is first divided into a search for two words vanishing, respectively, on *generating* and *non-generating* pairs of elements in our group $G$. The constructions of these two words are quite different. For generating pairs, we identify a large subset $E \subseteq G$ satisfying a short identity. For $G = \mathrm{Sym}(n)$, the set $E$ is the set of $n$-cycles; for $G$ of Lie type it is usually the union of split maximal tori. We then show that many short words in our generating pair of elements will lie in $E$, using results on mixing times and random walks in $G$ (see subsection 2.2) and compose these words with the identity holding in $E$.

A non-generating pair of elements lie in a common maximal subgroup $M$ of $G$. By classifying the possibilities for $M$ we can produce laws by induction. For $G = \mathrm{Sym}(n)$, this is facilitated by the O'Nan-Scott Theorem, and consequences thereof due to Liebeck (see [20] for details). To carry out the induction needed to prove Theorem 1.9 in full generality is a deep matter, requiring Aschbacher's Theorem on maximal subgroups of finite classical groups, the Classification of Finite Simple Groups, results on the classification of maximal subgroups in exceptional groups of Lie type, and dimension bounds for permutational and linear representations of finite simple groups. That said, to prove Theorem 1.1 we will only apply Theorem 1.9 in the case $G = \mathrm{PSL}_3(q)$ or $\mathrm{PSU}_3(q)$, for which the determination of maximal subgroups is classical (see [19]).

One common feature of the proofs of Theorems 1.1, 1.8 and 1.9 is the use of probabalistic arguments to demonstrate the existence of words with certain properties. That is, it is shown that, according to a certain model of random words, a word has the desired property with positive probability, and it is deduced that such a word must exist. As such, the proofs are non-constructive: they do not facilitate the description of explicit laws for the given groups. By contrast, Theorem 1.6 is constructive, and words $w_n$ satisfying the conclusions of that theorem could in principle be explicitly written down. It remains a beguiling question what the form of the words $w_n$ arising in Theorem 1.1 might be.

### 1.3 Outline of the Paper

In Section 2 we assemble some basic tools for constructing laws in groups (Subsection 2.1), material on mixing times and random walks in finite groups (Subsection 2.2), and notions relating to residual finiteness growth, including the deduction of Theorem 1.2 from Theorem 1.1 (Subsection 2.3).

The proof of Theorem 1.1, to which Section 3 is devoted, has much in common with that of Theorem 1.6 found in [24]. There, the problem of constructing a short law valid in *all* sufficiently small finite groups was first reduced to that of constructing a short law valid only in all sufficiently small *simple* groups. This reduction will also be the first step in the proof of Theorem 1.1. It is summarised in Subsection 3.1, and appears in full detail in [24]. Further standard reductions (discussed in Subsection 2.1) allow us to consider separately each of the eighteen infinite families of finite simple groups (since the bound in Theorem 1.1 is asymptotic, the sporadic groups are easily eliminated).

The key novelty of our work lies in our treatment of groups of the form $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ (for all other finite simple groups, the laws constructed in [24] suffice; this is explained in Subsection 3.2). Once again, we may consider these three classes separately from the other finite simple groups, and from each other. $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ are then easily dealt with using Theorem 1.9: we have a short law for each individual group and these can be combined over all sufficiently small $q$. This is carried out in Subsection 3.3.

By contrast, combining laws for individual groups of the form $\mathrm{PSL}_2(q)$ into one law valid for all of them is too expensive (essentially, there are too many such groups of small order). This issue provided the bottleneck for the bound in Theorem 1.6. Instead, we take an approach closer in spirit to that used in the *proof* of Theorem 1.9, as it was sketched in Subsection 1.2. Namely, given a generating pair in some $\mathrm{PSL}_2(q)$, we use random walks to locate many short words potentially satisfying a short relation. Those words are then combined using an iterated commutator to yield one word that works with high probability.

In contrast to previous work, however, we run random walks in pairs, and locate pairs of elements lying in a common Borel subgroup. Since there is a common law satisfied by the Borel subgroups of *every* $\mathrm{PSL}_2(q)$ (a double commutator), there is no need to combine laws for the individual groups: the words we produce using the random walk method will already provide laws holding simultaneously in $\mathrm{PSL}_2(q)$ for all sufficiently small $q$. This approach works as stated for a set of good primes arising from the work of Breuillard and Gamburd [5] on uniform expansion for $\mathrm{PSL}_2(p)$. This argument, the subject of Subsection 3.4, is the technical heart of our work. The groups $\mathrm{PSL}_2(q)$ for other primes, prime powers and other finite simple groups are dealt with by a more direct argument. The paper concludes with a short survey of open problems.

# 2 Preliminaries

## 2.1 Laws in Finite Groups

We start out with some basic definitions.

**Definition 2.1.** *Fix $x, y$ an ordered basis for the free group $F_2$ and let $w \in F_2 \setminus \{1\}$. For any group $G$ define the* evaluation map $G \times G \to G$ *(also denoted $w$) by $w(g,h) = \pi_{(g,h)}(w)$, where $\pi_{(g,h)}$ is the (unique) homomorphism $F_2 \to G$ extending $x \mapsto g$, $y \mapsto h$. We call $w$ a* law for $G$ *if $w(G \times G) = \{1_G\}$.*

Of course we could equally define word maps $G^k \to G$ associated to elements of $F_k$ for any $k \geq 1$, and thereby seek laws for $G$ within $F_k$, however it turns out that very little is lost by restricting to $k = 2$. For if $k > 2$, standard embeddings of $F_k$ into $F_2$ associate to every law $w \in F_k$ for $G$ a law $\tilde{w} \in F_2$ for $G$, of length depending linearly on the length of $w$, while conversely, an inclusion of a basis for $F_2$ into a basis for $F_k$ turns every law for $G$ in $F_2$ into a law in $F_k$. Meanwhile, a nontrivial element $w \in F_1 \cong \mathbb{Z}$ is a law for $G$ iff the exponent of $G$ divides $w$ (viewed as an integer).

We note two basic facts about the structure of laws in finite groups, which will enable us to construct new laws from old. The first allows us to combine words vanishing on subsets of a group to a new word vanishing on the union of those subsets, and is proved as Lemma 2.2 in [20]. To this end, recall for $G$ a group and $w \in F_2$ a word the definition of the *vanishing set* $Z(G, w)$ of $w$ on $G$ from [24]:

$$Z(G, w) = \{(g, h) \in G \times G \mid w(g, h) = 1_G\}.$$

**Lemma 2.2.** *Let $w_1, \ldots, w_m \in F_2$ be non-trivial words. Then there exists a non-trivial word $w \in F_2$ of length at most $16m^2 \max_i |w_i|$ such that for all groups $G$,*

$$Z(G, w) \supseteq Z(G, w_1) \cup \ldots \cup Z(G, w_m).$$

Note that, as well as allowing us to increase the vanishing set of words within a single group, Lemma 2.2 allows us to take a family of groups and, given a law for each group in the family, produce a new law which holds in every group in the family simultaneously.

The second fact allows us to construct laws for group extensions. It is proved as Lemma 2.2 in [24].

**Lemma 2.3.** *Let $1 \to N \to G \to Q \to 1$ be an extension of groups. Suppose $N, Q$ satisfy non-trivial laws in $F_2$ of length $n_N, n_Q$, respectively. Then $G$ satisfies a non-trivial law of length at most $n_N n_Q$.*

The previous lemma is stated in [24] with $n_N(n_Q + 2)$ in place of $n_N n_Q$, but the additional summand is easily removed.

**Example 2.4.** A group $A$ is abelian iff the word $x^{-1}y^{-1}xy \in F(x, y)$ is a law for $A$. By Lemma 2.3 and induction, it follows that if $G$ is soluble of derived length at most $d$, then $G$ satisfies a law of length at most $4^d$. Since every nilpotent group of class at most $2^d$ is soluble of derived length at most $d$, these groups also satisfy such a law.

The work of Elkasapy and the second author [9] on the derived and lower central series of $F_2$ allows one to construct even shorter laws for soluble and nilpotent groups, of which we will avail ourselves in the sequel.

## 2.2 Mixing times and Random Walks

Let $G$ be an finite group, and let $S \subseteq G$ be a symmetric generating set. We will consider a lazy random walk associated with the set $S$, as follows: let $x_1, \ldots, x_l$ be independent random variables, each with distribution function:

$$\tfrac{1}{2|S|}\chi_S + \tfrac{1}{2}\delta_{1_G}$$

where $\chi_S$ is the indicator function of $S$ and $\delta_{1_G}$ is the Dirac mass at the identity. Let $\omega_l$ be the random variable on $G$ given by $\omega_l = x_1 \cdots x_l$. We are interested in the mixing time of the random walk.

Seminal results about the mixing times of random walks on $\mathrm{PSL}_2(q)$ were derived from diameter bounds proved by Helfgott [13] (for the case $q$ prime) and generalizations (to arbitrary $q$) due to Dinai [8] and Varjú [25]. We are going to use the following result due to Breuillard and Gamburd [5] that holds for $\mathrm{PSL}_2(p)$ for a sufficiently large set of primes.

**Theorem 2.5** (Breuillard-Gamburd)**.** *There is a constant $\delta > 0$ such that for all all $n \geq 2$ the number of rational primes $p$ less than $n$ for which $\mathrm{PSL}_2(p)$ has uniform spectral gap less than $\delta$ is at most $n^{1/2}$.*

For sake of convenience, we will refer to the set of primes arising from the previous theorem as the set of good primes. Note that a spectral gap of $\delta$ just means that the spectral radius of the random walk acting on mean-zero functionals is bounded from above by $1 - \delta$ and thus, the random walk approaches equidistribution exponentially fast. We therefore have the following corollary.

**Corollary 2.6.** *Let $G = \mathrm{PSL}_2(p)$ and $p$ a good prime and let $S \subseteq G$ be a generating set and let $E \subseteq G$. Then:*

$$\mathbb{P}[\omega_l \in E] \geq |E|/2|G|$$

*for all $l \geq O(\log|G|)$.*

For more details on the relevant concepts and results consult [6].

## 2.3 Residual Finiteness Growth

We recall the definition of the *residual finiteness growth function* from the Introduction. Let $\Gamma$ be a finitely generated residually finite group and let $1_\Gamma \neq g \in \Gamma$. Define:

$$k_\Gamma(g) = \min\{|Q| \mid \text{there exists } \pi : \Gamma \to Q, \pi(g) \neq 1_Q\}.$$

Fix a finite generating set $S$ for $\Gamma$. For $n \in \mathbb{N}$:

$$\mathcal{F}_\Gamma^S(n) = \max\{k_\Gamma(g) \mid 1_\Gamma \neq g \in \Gamma, g \in B_S(n)\}.$$

Here $B_S(n)$ denotes the ball of radius $n$ with respect to the word metric associated with $S$. The function $\mathcal{F}_\Gamma^S$, known as the *residual finiteness growth function* for $\Gamma$ (with respect to $S$) was introduced and studied by Bou-Rabee [2], up to a natural notion of equivalence of functions.

**Definition 2.7.** *For any $f_1, f_2 : (0,\infty) \to (0,\infty)$, write $f_1 \preceq f_2$ if there exists $C > 0$ such that $f_1(x) \leq C f_2(Cx)$ for all $x \in (0,\infty)$, and write $f_1 \simeq f_2$ when both $f_1 \preceq f_2$ and $f_2 \preceq f_1$.*

It is clear from this definition that $\simeq$ is an equivalence relation. Of course any $f : \mathbb{N} \to (0,\infty)$ can be extended to $(0,\infty)$ via $f(x) = f(\lfloor x \rfloor)$. Such functions may thereby also be compared under $\preceq$.

**Lemma 2.8** ([2])**.** *Let $H$ be a subgroup of $\Gamma$ generated by a finite set $L$. Then $\mathcal{F}_H^L \preceq \mathcal{F}_\Gamma^S$.*

We conclude the following corollary.

**Corollary 2.9.** *Let $S, T$ be finite generating sets for $\Gamma$. Then $\mathcal{F}_\Gamma^S \simeq \mathcal{F}_\Gamma^T$. Thus we may speak without ambiguity about the ($\simeq$-class of the) residual finiteness growth function $\mathcal{F}_\Gamma$ of $\Gamma$ itself.*

Since any non-abelian finite-rank free group embeds into any other, we also obtain the following consequence.

**Corollary 2.10.** *Let $\Gamma_1, \Gamma_2$ be finite-rank free groups of rank $\geq 2$. Then $\mathcal{F}_{\Gamma_1} \simeq \mathcal{F}_{\Gamma_2}$.*

There is a close relationship between residual finiteness growth of free groups and laws for finite groups.

**Proposition 2.11.** *Let $\alpha : (0, \infty) \to (0, \infty)$ be a strictly increasing function. Suppose that for all $n$ there is a law of length at most $\alpha(n)$ simultaneously valid in all groups of order at most $n$. Let $\Gamma$ be a finite-rank free group. Then:*

$$\alpha^{-1} \preceq \mathcal{F}_\Gamma.$$

*Proof.* By Corollary 2.10 we may assume $\Gamma = F_2$. Fix a basis $S$ for $\Gamma$. Let $w \in \Gamma$ be a non-trivial word of length at most $\alpha(n)$, which is simultaneously a law for all groups of order at most $n$. Then $k_\Gamma(w) \geq n+1$, so $\mathcal{F}_\Gamma^S(\alpha(x)) \geq x$, for all $x \in (0, \infty)$. The claim now follows from Corollary 2.9. □

We may now complete:

*Proof of Theorem 1.2.* By Theorem 1.1 there exists $C > 0$ such that we may take $\alpha$ as in Proposition 2.11 with:

$$\alpha^{-1}(n) \geq n^{3/2}/C \log(n)^{9/2+\varepsilon}.$$

□

# 3 Proof of Theorem 1.1

## 3.1 Reduction to Simple Groups

As discussed above, the proof of Theorem 1.6 appearing in [24] begins by reducing the problem of constructing laws valid in *all* finite groups up to the order bound to that of constructing laws valid only in all finite *simple* groups up to the order bound. Via the same reductions, our Theorem 1.1 will follow from the following result, which improves asymptotically on Proposition 4.1 from [24].

**Proposition 3.1.** *For all $n \in \mathbb{N}$, there exists a word $w_n \in F_2$ of length:*

$$O\left(n^{2/3} \log(n)^3\right)$$

*such that for every finite* simple *group $G$ satisfying $|G| \leq n$, $w_n$ is a law for $G$.*

Theorem 1.1 follows from substituting Proposition 3.1 in place of Proposition 4.1 from [24], and proceeding *mutatis mutandis* with the argument as in [24]. We refer the reader there for the details (and in particular for references for many of the assertions made in the proof), and here restrict ourselves to an outline.

*Proof of Theorem 1.1 (sketch).* First suppose that $G$ is nilpotent. The bound $|G| \leq n$ implies the nilpotency class of $G$ is at most $\log_2(n) + 1$ (the maximal length of a subgroup chain in $G$). By Example 2.4, $G$ satisfies a law of length:

$$\log(n)^{O(1)}.$$

A more precise analysis using results from [9] yields a bound of $O(\log(n)^{3/2})$, see Proposition 3.1 in [24].

Now more generally assume $G$ is soluble. Let $N$ be the Fitting subgroup of $G$. Fix a prime $p$ and let $N(p)$ be the Sylow $p$-subgroup of $N$. The action of $\mathrm{Aut}(N(p))$ on the Frattini quotient of $N(p)$ (whose rank we denote by $m(p)$) induces a map $\alpha_p : \mathrm{Aut}(N(p)) \to \mathrm{GL}_{m(p)}(p)$, whose kernel is a $p$-group. Moreover the natural map $\psi : G \to \prod_p \mathrm{Aut}(N(p))$ is an embedding modulo the center of $G$. Since $\ker(\prod_p \alpha_p) \cap \psi(G)$ is nilpotent and by Lemma 2.3, it suffices to find a law for $\mathrm{im}((\prod_p \alpha_p) \circ \psi)$.

Since $G$ is soluble, so is its image in $\mathrm{GL}_{m(p)}(p)$. The derived length of the latter is $O(\log(m(p)))$. Note that, since $|G| \leq n$, $m(p) \leq \log_2(n)$. We apply the bound for laws in soluble groups from Example 2.4 to $\mathrm{im}((\prod_p \alpha_p) \circ \psi)$ Putting all this together, $G$ satisfies a law of length:

$$\log(n)^{O(1)}.$$

Again, a more precise analysis using the results of Elkasapy and the second author on the length of the shortest non-trivial element of in the $k$th step of the derived series $F_2^{(k)}$ [9] yields a bound of $O(\log(n)^{9/2})$, see Proposition 3.2 in [24]. Let's fix a constant $D_2 > 0$, such that there exists a word of length $D_2 \log(n)^{9/2}$, which is satisfied by each solvable group of size at most $n$.

Finally consider a general group $G$. Recall that every finite group is soluble-by-semisimple, so by Lemma 2.3 and the previous paragraph, we may assume $G$ is semisimple (in the sense of Fitting).

There exist finite simple groups $H_i$ and $k_i \in \mathbb{N}$ such that $G$ may be identified with a subgroup of $\prod_{i=1}^{l} G_{(H_i,k_i)}$, for finite groups $G_{(H_i,k_i)}$ satisfying:

$$H_i^{k_i} \leq G_{(H_i,k_i)} \leq \mathrm{Aut}(H_i) \wr \mathrm{Sym}(k_i),$$

and in such a way that each $H_i^{k_i} \leq G$. The bound $|G| \leq n$ implies upper bounds on $|H_i|$ and $k_i$. By Theorem 1.8 and Lemma 2.3, the problem is reduced to the construction of short laws for the $\mathrm{Aut}(H_i)$.

For $H$ a finite simple group, the solution to Schreier's Conjecture implies that $\mathrm{Aut}(H)/H$ is soluble of derived length at most 3. The result now follows from Proposition 3.1 and final applications of Lemma 2.3 and Lemma 2.2.

In total, having obtained a law of length $O(n^{2/3}\log(n)^3)$, valid for all simple groups up to size $n$, following the arguments in [24], we obtain a constant $D_1 > 0$ and laws of the length bounded by $D_1 n^{2/3}\log(n)^3$ valid for all semisimple groups of size up to $n$.

Consider now an increasing sequence of real numbers $a_1, \ldots, a_{L+1}$, where

$$a_1 := 1, \quad a_{k+1} = \exp\left(a_k^{4/27}\right)$$

and $L$ is the last index, where $a_L \leq n$. It is easy to see that $L = O(\log^*(n))$, where $\log^*$ denotes the iterated logarithm.

Now, let $G$ be a finite group of size at most $n$ and let $S \lhd G$ be its solvable radical with the associated semisimple quotient $G/S$. It is clear that there must exist some $j \in \{1, \ldots, L\}$ such that $|G/S| \leq n/a_j$ and $|S| \leq a_{j+1}$. Indeed, just take $j$ to be the last index with $|S| \geq a_j$.

Now, in each of the $L$ cases, Lemma 2.3 yields a law of length bounded by

$$D_1(n/a_j)^{2/3}\log(n/a_j)^3 \cdot D_2\log(a_{j+1})^{9/2} \leq D_1 D_2 n^{2/3}\log(n)^3,$$

that is valid for those $G$ that fall into this particular case. Combining all the $L = O(\log^*(n))$ cases using Lemma 2.2, we obtain a law of length

$$O\left(n^{2/3}\log(n)^3\log^*(n)^2\right)$$

that is valid for all groups of size at most $n$. Again, for details we refer to [24]. □

### 3.2 Reduction to Low-Rank Simple Groups of Lie Type

In fact, the only finite simple groups of Lie type for which the laws constructed in the proof of Proposition 4.1 from [24] do not already satisfy the requirements of Proposition 3.1 are those of the form $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$. That is, we reduce the proof of Proposition 3.1 to the following statement.

**Proposition 3.2.** *For all $n \in \mathbb{N}$, there exists a word $w_n \in F_2$ of length:*

$$O(n^{2/3})$$

*such that if $G$ is a finite simple group not of the form* $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$ *or* $\mathrm{PSU}_3(q)$ *for some prime power $q$, and $|G| \leq n$, then $w_n$ is a law for $G$.*

Roughly speaking, the reason these families provided the bottleneck for the length of laws in [24] was that they are the only families in which a finite simple group $G$ may contain an element $g$ of large order compared to the order of $G$.

*Proof of Proposition 3.1.* First assume $G$ to be a finite simple group of Lie type. We refer to the tables from [24] (p.5), which in turn are based on [16]. The tables record $a(G), b(G) \in \mathbb{N}$ such that, if $G$ is defined over a field of order $q$,

$$q^{a(G)} \ll |G| \quad \text{and} \quad \max_{g \in G} o(g) \ll q^{b(G)}$$

(with the implied constants absolute). Moreover by inspection of the tables, we may take $b(G) \leq 2/9 \cdot a(G)$ in all cases, except for when $G$ is of the form $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$ or $\mathrm{PSU}_3(q)$. Excluding the latter possibility, we have:

$$\max_{g \in G} o(g) \ll |G|^{2/9} \leq n^{2/9} \tag{1}$$

Meanwhile, a classical result of Landau shows that the maximal order of an element of $\mathrm{Alt}(k)$ is at most $\exp\left(O((k \log(k))^{1/2})\right)$, so $G = \mathrm{Alt}(k)$ also satisfies (1). Thus there exists an absolute constant $C > 0$ such that, if $G$ is a finite simple group other than $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$ or $\mathrm{PSU}_3(q)$, then:

$$G = \bigcup_{i=1}^{Cn^{2/9}} Z(G, x^i)$$

Applying Lemma 2.2 to the words $w_i = x^i$ for $1 \leq i \leq Cn^{2/9}$, we obtain a law of length $O(n^{2/3})$ valid simultaneously in all such $G$. Combining (by Lemma 2.2 again) this last law with the law obtained in Proposition 3.2, we obtain the required result. □

We will conclude by constructing, for each of the three families $\mathrm{PSL}_2(q)$, $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$, a law of the length $O(n^{2/3} \log(n)^3)$ valid in all groups in the family of order at most $n$, this is Proposition 3.4 and Proposition 3.11. The proof of Proposition 3.2, and hence of Theorem 1.1, is then completed by combining these three laws using Lemma 2.2.

### 3.3 Short Laws for $\mathrm{PSL}_3(q)$ & $\mathrm{PSU}_3(q)$

The required result for groups of the form $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ will be obtained by combining the laws produced by Theorem 1.9 as $q$ varies over all sufficiently small prime powers. To this end, we record the following standard consequence of the Prime Number Theorem (see [10]).

**Lemma 3.3.** *For any $n \in \mathbb{N}$, the number of prime powers at most $n$ is $O(n/\log(n))$, and the number of these which are proper powers of primes is $O(n^{1/2})$.*

**Proposition 3.4.** *For all $n \in \mathbb{N}$, there exists a word $w_n \in F_2$ of length:*

$$n^{3/8}\log(n)^{O(1)}$$

*such that if $G$ is equal to $\mathrm{PSL}_3(q)$ or $\mathrm{PSU}_3(q)$ for some prime power $q$, and $|G| \leq n$, then $w_n$ is a law for $G$.*

*Proof.* First note that $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ satisfy the conditions of Theorem 1.9 with $d = 3$, so satisfy laws of length $q^{\lfloor 3/2 \rfloor}\log(q)^{O(1)} = q\log(q)^{O(1)}$.

Alternatively and without using the results of [4], we could have studied the orders of elements in $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ more carefully and noted that the order of each element divides $q^2-q, q^2+q, q^2-1, q^2+q+1$ or $q^2-q+1$. Using Lemma 2.2, this implies immediately that there is a law of length $O(q^2)$ satisfied by these groups – enough for us to proceed.

Recall that $\mathrm{PSL}_3(q)$ and $\mathrm{PSU}_3(q)$ have order proportional to $q^8$, so if $G$ is isomorphic to some $\mathrm{PSL}_3(q)$ or $\mathrm{PSU}_3(q)$ and $|G| \leq n$, then $q = O(n^{1/8})$. By Lemma 3.3, there are $O(n^{1/8}/\log(n))$ such prime powers $q$.

We may thus apply Lemma 2.2 with $m = O(n^{1/8}/\log(n))$ and $w_i$ of length $n^{1/8}\log(n)^{O(1)}$ (or merely $O(n^{1/4})$ using the alternative argument) to obtain a law of length $n^{3/8}\log(n)^{O(1)}$ (or just $O(n^{1/2}/\log(n)^2)$ on the alternative route) valid in all groups of the required form. □

### 3.4 Short Laws for $\mathrm{PSL}_2(q)$

Observe first that the argument of the previous subsection necessarily fails for $\mathrm{PSL}_2(q)$. For let $u_q$ be a law for $\mathrm{PSL}_2(q)$. Then $u_q$ has length $\Omega(q)$ (see [12]). Combining the laws $u_q$ by Lemma 2.2 over all values of $q$ such that $|\mathrm{PSL}_2(q)| \leq n$ (that is, for $q = O(n^{1/3})$) would yield a law of length $\Omega(n/\log(n)^2)$, which is unacceptable for our purposes. However, this general strategy will be the way to treat prime powers and primes in the set of bad primes arising from Theorem 2.5 (recall that *good* and *bad primes* were defined in Subsection 2.2).

**Lemma 3.5.** *For all $n \in \mathbb{N}$ there exists a word $w_n \in F_2$ of length bounded by $O(n^{2/3})$ such that for $\mathrm{PSL}_2(q)$ with $q$ is either a proper prime power or a bad prime and satisfying $|\mathrm{PSL}_2(q)| \leq n$, $w_n$ is a law for $\mathrm{PSL}_2(q)$.*

*Proof.* The size of $\mathrm{PSL}_2(q)$ is about $q^3$ so that we have to consider prime powers up to size $O(n^{1/3})$. The size of the set of proper prime powers and bad primes below $O(n^{1/3})$ is bounded by $O(n^{1/6})$, see Lemma 3.3. It is well-known that laws of length $O(n^{1/3})$ for $\mathrm{PSL}_2(q)$ exist (see the proof of Proposition 4.1. in [24]). Combining all these laws yields the desired law using Lemma 2.2 of length $O(n^{2/3})$. □

We are now left to deal with groups $\mathrm{PSL}_2(q)$ where $q$ is a good prime. We divide the problem and seek separately short words whose associated vanishing sets contain, respectively, generating and non-generating pairs of elements in groups of the form $\mathrm{PSL}_2(q)$. The strategy in both cases closely parallels that employed in the proofs of Theorems 1.8 and 1.9.

For generating pairs we will use upper bounds on the mixing time of $\mathrm{PSL}_2(q)$ arising from Theorem 2.5. This allows us to give a probabalistic construction of pairs of words, whose evaluation maps have images contained in a common soluble subgroup of $\mathrm{PSL}_2(q)$ (and hence satisfy a short relation). For non-generating pairs we use the classification of subgroups of $\mathrm{PSL}_2(q)$.

We start by recording an elementary observation from linear algebra.

**Lemma 3.6.** *The number of elements of $\mathrm{SL}_2(q)$ which are diagonalisable over $\mathbb{F}_q$ is $\Omega(q^3)$.*

Since the order of $\mathrm{SL}_2(q)$ is proportional to $q^3$, Lemma 3.6 says precisely that an absolutely positive proportion of elements are diagonalisable over $\mathbb{F}_q$. Now consider the subgroup $U(q) \leq \mathrm{SL}(q)$ of upper-triangular elements. $U(q)$ contains the diagonal subgroup of $\mathrm{SL}_2(q)$, so by Lemma 3.6, an absolutely positive proportion of the elements of $\mathrm{SL}_2(q)$ are conjugate into $U(q)$.

By a *Borel subgroup* of $\mathrm{PSL}_2(q)$ we shall mean the image, under the natural projection $\mathrm{SL}_2(q) \to \mathrm{PSL}_2(q)$, of a conjugate in $\mathrm{SL}_2(q)$ of $U(q)$. This is not really the "right" way to define these subgroups, but it is the most convenient for our purposes. The only facts we require about Borel subgroups in the sequel are:

($a$) Every Borel subgroup is metabelian;

($b$) Every Borel subgroup has index $\ll q$ in $\mathrm{PSL}_2(q)$;

(*c*) A positive proportion of the elements of $\mathrm{PSL}_2(q)$ lie in a Borel subgroup

Indeed, (*a*) and (*b*) are well-known and (*c*) is just the summary of the preceding discussion.

We shall also require some facts about free groups. The first of these is standard.

**Lemma 3.7** (see for instance [15] Chapter 1)**.** *Let $a, b \in F_2$. Then either*

(*i*) *$a$ and $b$ commute, and are powers of a common element of $F_2$, or*

(*ii*) *the subgroup $\langle a, b\rangle$ of $F_2$ generated by $a$ and $b$ is isomorphic to $F_2$, and $\{a, b\}$ is a free generating set.*

We further recall Kesten's result on the exponential decay of simple random walks on $F_2$.

**Theorem 3.8** ([18])**.** *There exists a constant $\alpha > 0$ such that, for any $g \in F_2$, if $w_l$ is the result of a simple random walk of length $l$ on a free generating set for $F_2$,*

$$\mathbb{P}[w_l = g] \ll \exp(-\alpha l).$$

The key consequence of these two facts that we shall use is the following, which tells us that with high probability, the outcomes of a pair of random walks on $F_2$ fall into case (ii) of Lemma 3.7, see also [5, Lemma 2.1].

**Corollary 3.9.** *Let $\alpha > 0$ be as in Theorem 3.8. Let $u_l, v_l$ be the results of two independent simple random walks of length $l$ on a free generating set for $F_2$. Then:*

$$\mathbb{P}\big[[u_l, v_l] = 1\big] \ll l \exp(-\alpha l).$$

*Proof.* It is a basic fact that $v = w^k$ in $F_2$ for some non-trivial $w$ implies that the word length of $v$ is at least $k$. Moreover, it follows from Lemma 3.7 that each non-trivial $u \in F_2$ lies in a unique maximal abelian subgroup, which is isomorphic to $\mathbb{Z}$ – generated by some maximal root $w$ of $u$. Thus, for any fixed $u_l$ of length at most $l$, there is a maximal root $w_l$ and $[u_l, v_l] = 1$ with $v_l$ of length at most $l$ implies $v_l = w_l^k$ for some $k \in \mathbb{N}$ satisfying $-l \leq k \leq l$ by Lemma 3.7. Hence, as long as $u_l$ is non-trivial, the probability that $v_l$ satisfies $[u_l, v_l] = 1$ is bounded by $O(l \exp(-\alpha l))$. However, the probability that $u_l$ is trivial is bounded by $O(\exp(-\alpha l))$. This proves the claim. □

Finally, we record a taxonomy of the subgroups of $\mathrm{PSL}_2(q)$, which follows from the classical results of Dickson [7] (see also [19]).

**Theorem 3.10** (Dickson)**.** *Let $q$ be a prime and let $H$ be a proper subgroup of $\mathrm{PSL}_2(q)$. Then one of the following holds.*

(*i*) *$H$ is metabelian;*

(*ii*) *$|H| \leq 60$.*

We have arrived at the heart of the proof – our new approach to treat the crucial case $\mathrm{PSL}_2(q)$.

**Proposition 3.11.** *For all $n \in \mathbb{N}$, there exists a word $w_n \in F_2$ of length:*

$$O\left(n^{2/3}\log(n)^3\right)$$

*such that if $G$ is equal to $\mathrm{PSL}_2(q)$ for some prime power $q$, and $|G| \leq n$, then $w_n$ is a law for $G$.*

*Proof.* Let $u_1, \ldots, u_m, v_1, \ldots, v_m$ be the results of $2m$ independent lazy random walks of length $l = C_1 \log(n)$ on a free generating set for $F_2$, where $C_1$ is a sufficiently large absolute constant. Fix (for the time being) a good prime $q$ such that $|\mathrm{PSL}_2(q)| \leq n$ and a generating pair $g, h \in \mathrm{PSL}_2(q)$.

For each $1 \leq i \leq m$, the probability that $u_i(g,h)$ lies in a Borel subgroup is at least a positive absolute constant $C_2$, by Lemma 3.6 and Corollary 2.6 (since we are assuming $C_1$ is sufficiently large, Corollary 2.6 is indeed applicable).

Suppose $u_i(g,h)$ does indeed lie in a Borel subgroup $B(q) \leq \mathrm{PSL}_2(q)$. By independence of $u_i$ and $v_i$, and applying Corollary 2.6 again, the probability that $v_i(g,h)$ lies in $B(q)$ is at least $1/C_3 q$, for an absolute constant $C_3 > 0$. Thus the probability that $u_i(g,h)$ and $v_i(g,h)$ do not lie in a common Borel subgroup is at most

$$1 - C_2/C_3 q \leq 1 - C_2/C_3 n^{1/3}.$$

By independence of the $u_j, v_j$, the probability that for every $1 \leq j \leq m$ the pair $(u_j(g,h), v_j(g,h))$ fail to lie in a common Borel subgroup is at most $(1 - C_2/C_3 n^{1/3})^m$. Setting $m = C_4 n^{1/3}\log(n)$, for $C_4$ a sufficiently large constant, we have

$$(1 - C_2/C_3 n^{1/3})^m \leq \exp(-C_5 \log(n)) = n^{-C_5}$$

for $C_5$ a constant, which we may take to be arbitrarily large.

The number of possible generating pairs $(g,h)$ for $\mathrm{PSL}_2(q)$ is no more than $|\mathrm{PSL}_2(q)|^2 \leq n^2$, while the number of possibilities for $q$ is bounded by $O(n^{1/3}/\log(n))$, using Lemma 3.3. Thus, taking a union bound over all possible good primes $q$ and $(g,h)$, the probability of the event: "for every $1 \leq j \leq m$ there exists a generating pair $g,h$ for some $\mathrm{PSL}_2(q)$ of order at most $n$ such that the pair $(u_j(g,h), v_j(g,h))$ fails to lie in a common Borel subgroup" is at most:

$$O\left(n^{7/3-C_5}/\log(n)\right) \tag{2}$$

We will choose $C_5 > 7/3$.

Meanwhile, by Corollary 3.9, for fixed $i$ the probability that $u_i$ and $v_i$ commute (in $F_2$) is $O(l\exp(-\alpha l))$, so taking a union bound, the probability that there exists $1 \leq i \leq m$ such that $u_i$ and $v_i$ commute is:

$$O(ml\exp(-\alpha l)) = O\left(n^{1/3-\alpha C_1}\log(n)^2\right) \tag{3}$$

(of course, we could get a better bound by using the independence of the pairs $(u_i, v_i)$, but (3) will prove more than adequate for our current needs).

Combining (2) and (3), the probability of the event "either there exists $1 \leq i \leq m$ such that $u_i$ and $v_i$ commute or for every $1 \leq i \leq m$ there exists a generating pair $g,h$ for some $\mathrm{PSL}_2(q)$ of order at most $n$ such that the pair $(u_j(g,h), v_j(g,h))$ fails to lie in a common Borel subgroup" is at most:

$$O\left(n^{7/3-C_5}/\log(n) + n^{1/3-\alpha C_1}\log(n)^2\right) < 1$$

for $C_1 > 1/\alpha$, $C_5 > 7/3$ and $n$ larger than an absolute constant.

Therefore there exist *deterministically* words $u_1, \ldots, u_m, v_1, \ldots, v_m \in F_2$ with $m = O(n^{1/3}\log(n))$ of length at most $l = O(\log(n))$ such that no pair $u_i, v_i$ commutes in $F_2$, and such that for every $\mathrm{PSL}_2(q)$ of order at most $n$, where $q$ is a good prime, and every generating pair $g,h \in \mathrm{PSL}_2(q)$, there exists $1 \leq i \leq m$ for which $(u_i(g,h), v_i(g,h))$ lie in a common Borel subgroup.

Consider the word $\tilde{w} = [[a,b],[b,a^{-1}]] \in F(a,b)$. It is easy to see that $\tilde{w}$ is a non-trivial element of $F(a,b)^{(2)}$ of length 14. Thus, on the one hand $w_i = \tilde{w}(u_i, v_i) \in F_2$ is non-trivial for every $1 \leq i \leq m$, since by Lemma 3.7 $u_i, v_i$ freely generate a group isomorphic to $F(a,b)$. On the other hand, since every Borel subgroup of $\mathrm{PSL}_2(q)$ is metabelian, for every $\mathrm{PSL}_2(q)$ of order at most $n$, where $q$ is a good prime, and every generating pair $g,h \in \mathrm{PSL}_2(q)$, there exists $1 \leq i \leq m$ for which

$$w_i(g,h) = \tilde{w}(u_i(g,h), v_i(g,h)) = 1.$$

Applying Lemma 2.2 to the words $w_1, \ldots, w_m$, we obtain a word $w_{gen} \in F_2$ of length bounded by

$$16(C_4 n^{1/3} \log(n))^2 \cdot (14 \cdot C_1 \log(n)) = O(n^{2/3} \log(n)^3),$$

which vanishes at all such generating pairs $g, h$.

Finally we produce a word of bounded length whose vanishing set contains all non-generating pairs. This will be achieved using Theorem 3.10. Indeed, if $g, h$ generate a metabelian subgroup or a group of bounded order (conclusions (i) or (ii) of Theorem 3.10), then $(g, h)$ lies in the vanishing set of a word of bounded length $w_{sub}$. Applying Lemma 2.2 one more time, to $w_{gen}, w_{sub}$ and the law obtained from Lemma 3.5 to cover also the case when $q$ is a proper prime power or a bad prime, we have the required result. □

# 4 Open Problems

We end this article with various possibly approachable open problems. At the moment, our constructions (or rather proof of existence) of laws are inherently random and say only very little about the shape of these elements in the free group.

**Problem 4.1.** *Give an explicit construction of short laws holding in:*

(*a*) *symmetric groups;*

(*b*) *finite simple groups of Lie type;*

(*c*) *all groups of order at most n (improving on Theorem 1.6).*

It remains plausible that there could exist laws of polynomial length for $\mathrm{Sym}(n)$. Note that assuming Babai's Conjecture saying that $\mathrm{diam}(\mathrm{Sym}(n))$ should be $n^{O(1)}$ (see [1]), Kozma and the second named author showed in [20] that laws of $\mathrm{Sym}(n)$ of length $n^{O(\log\log(n))}$ exist. Maybe a refined argument could also prove a polynomial bound assuming Babai's Conjecture. Based on existing polynomial diameter estimates for random generators of $\mathrm{Sym}(n)$ [14], words in $F_2$ of length $n^8 \log(n)^{O(1)}$ can be constructed that are laws for *almost all* of $\mathrm{Sym}(n)$, see [26]. Following [26], there exist similar improved bounds for *almost laws* of finite simple groups of Lie type. Indeed, for example the group $\mathrm{SL}_d(q)$ satisfies an almost law of length $q \log(q)^{O_d(1)}$. This will be explained in more detail in [4, 26].

**Problem 4.2.** *Give new upper bounds on the length of the shortest law for* $\mathrm{Sym}(n)$. *Can there be laws of length bounded by* $n^{O(1)}$*?*

On the other side, lower bounds are equally interesting.

**Problem 4.3.** *Give new lower bounds on the length of the shortest law for* $\mathrm{Sym}(n)$*, say of the form* $\Omega(n\log(n))$ *or* $\Omega(n^2)$*.*

Note that $\mathrm{PSL}_2(q) \subseteq \mathrm{Sym}(n)$ for $q < n$, so that a sharp complementary bound in Theorem 1.1 following the strategy by Kassabov-Matucci (see ([17, Remark 9] and the remarks after Theorem 1.2), would potentially also prove $\Omega(n^2)$ with respect to the previous problem. As regards a possible result complementary to Theorem 1.1, even a bound of $\Omega(n^{1/3}\log(n))$ would be an improvement to the state of the art.

**Problem 4.4.** *Give an improved upper bound on* $\mathcal{F}^S_{F_k}(n)$*, smaller than* $O(n^3)$*, for* $k \geq 2$*.*

A strengthening of Problem 4.3 is the following, which already seems very achievable.

**Problem 4.5.** *Find a generating set* $X_n$ *of* $\mathrm{Sym}(n)$ *such that the associated Cayley graph has girth* $\Omega(n\log(n))$*.*

Again, the best construction of generating sets of $\mathrm{Sym}(n)$ with respect to Problem 4.5 is random in nature and yields a bound on the girth of $\Omega((n\log(n))^{1/2})$, see [11, Thm. 3]. We are not aware of an explicit family of sets of generators satisfying this lower bound on the girth. The authors of [11] conjecture a positive answer to Problem 4.5 for random generators.

Needless to say, the exact determination the of the length and shape of shortest laws for symmetric groups or all finite group up to a certain size remains an outstanding open problem in finite group theory.

## Acknowledgements

The first named author wishes to thank the Institut für Geometrie of the Technische Universität Dresden for providing him with a hospitable welcome on the occasion of his visit in June 2016, during which the essence of the proof of Theorem 1.1 was first distilled. This research was supported by ERC Starting Grant No. 277728 and ERC Consolidator Grant No. 681207.

We thank the unknown referee for interesting comments that led us to include a refined version of our main result.

## References


[1] L. Babai and Á. Seress. *On the diameter of Cayley graphs of the symmetric group.* J. Combinatorial Theory-A 49 (1988), 175-179.

[2] K. Bou-Rabee. *Quantifying residual finiteness.* J. Algebra 323 (2010), 729-737

[3] K. Bou-Rabee and D.B. McReynolds. *Asymptotic growth and least common multiples in groups.* Bull. Lond. Math. Soc. 43 (2011) no. 6, 1059-1068

[4] H. Bradford and A. Thom. *Short laws for finite groups of Lie type.* In preparation.

[5] E. Breuillard and A. Gamburd. *Strong uniform expansion in SL(2,p).* Geom. Funct. Anal. 20 (2010), no. 5, 1201–1209.

[6] P. Diaconis and L. Saloff-Coste. *Comparison techniques for random walk on finite groups.* Ann. Probab. 21, Issue 4 (1993), 2131-2156

[7] L.E. Dickson. *Linear groups, with an Exposition of the Galois Field Theory.* Teubner, Leipzig, 1901.

[8] O. Dinai. *Growth in* $\mathrm{SL}_2$ *over finite fields.* J. Group Theory 14, Issue 2 (2011), 273–297

[9] A. Elkasapy and A. Thom. *On the length of the shortest non-trivial element in the derived and the lower central series.* J. Group Theory 18, Issue 5 (2015), 793-804

[10] P. Erdős and J. Surányi. *Topics in the Theory of Numbers.* Springer Science and Business Media, New York (2003)

[11] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, and B. Virág. *On the girth of random Cayley graphs.* Random Structures Algorithms 35 (2009), no. 1, 100–117.

[12] U. Hadad. *On the shortest identity in finite simple groups of Lie type.* J. Group Theory 14 (2011) no. 1, 37-47

[13] H. Helfgott. *Growth and Generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Ann. Math. 167 (2008) 601–623

[14] H. Helfgott, Á. Seress, and A. Zuk. *Random generators of the symmetric group: diameter, mixing time and spectral gap.* J. Algebra 421 (2015), 349–368.

[15] D.L. Johnson. *Presentations of Groups.* Cambridge University Press (1997)

[16] W. Kantor and A. Seress. *Large element orders and the characteristic of Lie-type simple groups.* J. Algebra 322 (2009), 802-832

[17] M. Kassabov and F. Matucci. *Bounding the residual finiteness of free groups.* Proc. Amer. Math. Soc. 139 (2011) no. 7, 2281-2286

[18] H. Kesten. *Symmetric random walks on groups.* Trans. Amer. Math. Soc. 92 (1959), Issue 2, 336-354.

[19] O.H. King. *The subgroup structure of finite classical groups in terms of geometric configurations.* Surveys in combinatorics, 2005. Edited by B. S. Webb.

[20] G. Kozma and A. Thom. *Divisibility and laws in finite simple groups.* Math. Ann. 361, Issue 1 (2016), 79-95

[21] B.H. Neumann. *Identical Laws in Groups I.* Math. Ann. 114, Issue 1 (1937), 506-525

[22] H. Neumann. *Varieties of Groups.* Springer Berlin Heidelberg (1967)

[23] I. Rivin. *Geodesics with one self-intersection, and other stories.* Adv. Math. 231 (2012), no. 5, 2391–2412.

[24] A. Thom. *About the length of laws for finite groups.* Isr. J. Math. (2017) 219, Issue 1, 469–478.

[25] P.P. Varjú. *Expansion in* $\mathrm{SL}_d(\mathcal{O}_K/I)$*, I square-free.* J. Eur. Math. Soc. 14 (2012), no. 1, 273–305

[26] C. Zyrus. *Almost laws for finite simple groups.* PhD Thesis, in preparation.

H. Bradford, Georg-August-Universität Göttingen, Germany
*E-mail address:* henry.bradford@mathematik.uni-goettingen.de

A. Thom, TU Dresden, Germany
*E-mail address:* andreas.thom@tu-dresden.de